N94- 29662

TDA Progress Report 42-116

February 15, 1994

Convolutional Encoding of Self-Dual Codes

G. Solomon[1]

There exist almost complete convolutional encodings of self-dual codes, i.e., block codes of rate 1/2 with weights w, w = *0 mod 4. The codes are of length 8*m *with the convolutional portion of length 8*m−*2 and the nonsystematic information of length 4*m−*1. The last two bits are parity checks on the two (4*m−*1) length parity sequences. The final information bit complements one of the extended parity sequences of length 4*m*. Solomon and van Tilborg [1] have developed algorithms to generate these for the Quadratic Residue (QR) Codes of lengths 48 and beyond. For these codes and reasonable constraint lengths, there are sequential decodings for both hard and soft decisions. There are also possible Viterbi-type decodings that may be simple, as in a convolutional encoding/decoding of the extended Golay Code [2]. In addition, the previously found constraint length* K = *9 for the QR (48, 24;12) Code is lowered here to* K = *8. In future articles, we shall search for candidates with small* K *constraint lengths for the (80,40;16) Quadratic Residue Code or some isomorph.*

I. Technique

There exist almost complete convolutional encodings of self-dual codes, i.e., block codes of rate 1/2 with weights $w, w = 0 \bmod 4$. A new technique applied here is to generate convolutional codes of lengths $2(4m - 1)$ using specifically related irreducible polynomials to give a tail-bitten block code of distance $d - 2$. Adjoining an additional information bit that complements one of the sequences of length $(4m - 1)$ and then appending two bits of parity on these individual $(4m - 1)$ sequences, one obtains an $(8m, 4m; d)$ code where all code words have weights that are multiples of 4. The minimum distance d will be optimal or near optimal for binary codes of rate 1/2 and length $8m$, if the polynomials have been chosen well.

Let $n = 4m - 1$. We choose the polynomials $p(x)$ and $q(x)$ to be taps of a convolutional encoder of K stages. We feed in a sequence of $n + K - 1$ information bits to the encoder with the first and last $(K - 1)$ bits the same. This generates a $(2n, n; d)$ block code. We append two additional parity checks on the two sequences of length

[1] Independent consultant to the Communications Systems Research Section.

n. A final information bit is modulo two added to the sequence generated by one of the polynomials, say $p(x)$. The final result is an $(8m, 4m; d)$ code.

Notice that this definition of the code differs from the one in the preceding paragraph. Clearly it does not matter in which order the parity checks are appended and the final information bit is added. For certain proofs, one definition will be preferable. The choice of $p(x)$ and $q(x)$ guarantees the even weights of the convolutionally encoded portion to be multiples of 4. The last two parity bits and the choice of the lengths guarantee that all weights of the code will be multiples of 4. This will be proven in the next section using the Solomon–McEliece Γ_2 formula. (See [3].)

In order to compute d, choose an irreducible polynomial $p(x)$ of degree $K - 1$ that is relatively prime to $x^n + 1$. Define $q(x) = x^{K-1}p(x^{-1})$. Find $p(x)/q(x) \equiv f(x) \pmod{x^n + 1}$. Test for the distance d relative to the total length of the convolutionally generated $(2n, n; d)$ code.

II. A Construction Theorem

For any positive integer $m \geq 3$, let $n = 4m - 1$. We may construct a block code of rate 1/2 of length $2(n+1) = 8m$ so that

(1) All of the weights are multiples of 4.

(2) The portion of length $2n$ is convolutionally generated by a K stage register $p(x)$ and $q(x)$ of degree $K - 1$ whose entries are $n + K - 1$ bits long with the first and last $(K - 1)$ bits identical. Two parity sequences, each of length n, are nonsystematically generated, one for each polynomial.

(3) The $(n + 1)$th information bit is added to each bit of the $p(x)$ parity sequence.

(4) The last 2 bits are overall parity checks on the n bit parity sequences.

(5) The minimum distance $d = 4d'$ is determined by the encoder polynomials $p(x)$ and $q(x)$ of degree $K - 1$. The polynomials are related thus: $q(x) = x^{K-1}p(x^{-1})$.

(6) $p(x)$ is chosen to give the maximum Hamming distance possible for the lengths $2(n+1)$. For example, it is shown in [1] that a $p(x)$ with $K = 9$ can be used to construct the (48,24;12) Quadratic Residue Code. This is improved to $K = 8$ here.

Proof: Let us examine the parity sequences of lengths $n = 4m - 1$ generated by $p(x)$ and $q(x)$ of degree $K - 1$. These are of the form $I(x)p(x) \pmod{x^n + 1}$ and $I(x)q(x) \pmod{x^n + 1}$. We shall obtain the Mattson–Solomon (MS) representation for the code word above. Let c_i be the MS coefficients of the information sequence $I(x)$ of length $n = 4m - 1$. For a suitably chosen z, $c_i = \sum_{j=0}^{(n-1)} a_j z^{-ij}$, where z is a primitive nth root of unity and a_i is the information sequence associated with $I(x)$. Then we get $c_i p(z^{-i})$ and $c_i q(z^{-i})$ for the MS coefficients of the parity sequences $I(x)p(x) \pmod{x^n + 1}$ and $I(x)q(x) \pmod{x^n + 1}$.

If $c_o = 0$, both the parity sequences have even weight and the even weights mod 4 are given by the Solomon–McEliece Γ_2 formula. If d_i are the MS coefficients, then $\Gamma_2 = \sum_{i=0}^{(n-1)/2} d_i d_{n-i}$. For the $p(x)$ parity sequence, this gives

$$\Gamma_2 = \sum_{i=0}^{(n-1)/2} c_i p(z^i) c_{-i} p(z^{-i})$$

For the $q(x)$ parity sequence, one obtains

$$\Gamma_2 = \sum_{i=0}^{(n-1)/2} c_i q(z^i) c_{-i} q(z^{-i})$$

Using the relationship of $p(x)$ to $q(x)$, one obtains equality of Γ_2 for the two sequences. Thus, the weights mod 4 are the same for the two parity sequences, and the sum of the weights mod 4 is therefore zero. This conclusion is unchanged when the two overall parity checks are appended to the convolutionally encoded parity sequences because, for this case, the parity checks are both zero. Finally, when the nth information bit is added to the $p(x)$ parity sequence of full length $4m$, the weight mod 4 is also unchanged. Thus, the total weight sum in this case is again a multiple of 4.

The odd weights of the parity sequences are generated by complementing the even-weight words. Consider the all-one $I(x)$ with only $c_0 = 1$. This yields two all-one parity sequences. Appending the overall parity checks to both gives two all-one vectors of length $2(n+1) = 8m$. All odd weights extended by even parity are thus transformed now to even weights divisible by 4.

From Solomon–van Tilborg [1], one obtains for $m = 3$ the Golay Code with $K = 4$ and $p(x) = x^3 + x + 1$. For

$m = 6$, one obtains the (48,24;12) Quadratic Residue Code with $K = 9$ and $p(x) = x^8 + x^4 + x^3 + x + 1$.

III. New Construction of the (48, 24;12) Quadratic Residue Code

In this section, we introduce an improved construction of the (48,24;12) Quadratic Residue (QR) Code that requires a convolutional encoding with $K = 8$ instead of $K = 9$.

Let $n = 23, K = 8$, $p(x) = x^7 + x^6 + x^5 + x^2 + 1$, and $q(x) = x^7 + x^5 + x^2 + x + 1$. One obtains the QR (48,24;12) Code in the following manner.

A. Encoding

Let the information bits be $i(0)$, $i(1)$, $i(2)$, $i(3)$, ..., $i(22)$, $i(\infty)$. Extend this sequence 7 bits backward by defining $i(-j) = i(23 - j); j = 1, 2, \ldots, 7$.

The encoded bits are $b(j)$, $c(j)$, $j = 0, 1, \ldots, 23$, where for $j = 0, 1, \ldots, 22$,

$$b(j) = i(j-7) + i(j-6) + i(j-5) + i(j-2) + i(j) + i(\infty)$$

$$c(j) = i(j-7) + i(j-5) + i(j-2) + i(j-1) + i(j)$$

$$b(23) = \sum_{j=0}^{22} b(j)$$

$$c(23) = \sum_{j=0}^{22} c(j)$$

Transmit the sequence $b(j), c(j); 0 \le j \le 23$.

Thus, a (46,22;10) tail-biting convolutional code is transmitted, initiated by a 7-bit sequence that repeats after 16 more. To these two parity sequences are adjoined overall parity checks. The 24th information bit of the QR Code determines whether the $b(j)$ sequence is complemented. The above sequence is the (48,24;12) Quadratic Residue Code.

To see this, let the additive recursion or check polynomial for the code be given in powers of x by 0, 1, 4, 6, 9, 12, 13, 15, 16, 19, 20, 24. This generates the (47,24;11) code, with the additional 48th bit the overall parity check. This gives the proper rate 1/2 and the distance = 12.

There exist a code word at coordinates 0, 2, 5, 6, 7, 13, 15, 22, 23, 28, 37 (in powers of, say, β, a 47th root of unity) and the overall parity check bit. Identify the quadratic residues with the trace one elements and the nonquadratic residues as the trace zero elements. If we take $x = 1$, the 0th power coordinate, as the overall parity check on the other 23 trace one elements, and $x = 0$, the additive identity in the field $GF(2^{23})$, as the overall parity check on the 23 trace zero elements, there are 5 coordinates in each set. In the trace one elements, choosing β so that $\mathrm{Tr}\beta = 1$, one has coordinates 2, 6, 7, 28, 37. In the trace zero elements, the powers or coordinates that occur are 5, 13, 1, 5, 22, 23. The powers of 2 are 1 2 4 8 16 32 17 34 21 42 37 27 7 14 28 9 18 36 25 3 6 12 24. In powers of 4, starting with 37, one gets (37 7 28 18 25 6 24 2 8 32 34 42 27 14 9 36 3 12 1 4 16 17 21). Similarly, the nonquadratic residues in powers of 4, starting with 22, are (22 41 23 45 39 15 13 5 20 33 38 11 44 35 46 43 31 30 26 10 40 19 29). Note that if we choose $p(x) = x^7 + x^5 + x^2 + x + 1$ and $q(x) = x^7 + x^6 + x^5 + x^2 + 1$, this will generate a convolutional portion of length 46 and, adding the overall parity checks, this will yield the QR Code. Thus, $K = 8$.

Note $p(x)/q(x) \pmod{x^{23} + 1} = x^{20} + x^{19} + x^{17} + x^{16} + x^{14} + x^{12} + x^{10} + x^6 + x^3$. This implies that the following positions form a code word: 37, 45, 13, 38, 44, 46, 31, 30, 10, 40, 0, $x = 0$ (the additive identity).

Cyclically shifting from 30 on, one obtains a code word in code coordinates starting from 0: [0, 1, 7, 8, 10, 14, 15, 16, 17, 27, 30].

IV. Viterbi Decoding

The following is a procedure for decoding the convolutionally encoded self-dual code based on Viterbi decoding. First, we decode assuming that the 24th information bit is 0, i.e., the received length 23 $(p(x), q(x))$ parity sequences are usable for the Viterbi decoding. One needs only to guess or know the initial 7 bits and one can apply Viterbi

decoding using tail-biting techniques or try all 128 possible initial 7-tuples.

If one does not know the initial 7 bits, one may take the received encoded sequences (assuming that the 24th information bit is 0) and concatenate them until they form a chain of about 3 or 4 and then Viterbi decode as if starting in the middle. We use the parity information and take advantage of Hamming distance 12.

Alternatively, assume that the $p(x)$ sequence has been complemented and so concatenate the parity sequences $(1+p(x), q(x))$ to a length of 3 or 4, i.e., 69 or 92 bits, and Viterbi decode.

V. Future Work

In encoding and decoding the (80.40;16) extended QR Code, one uses the (78,39;14) tail-biting convolutional subcode. We shall try to find the smallest constraint length K for which our construction will work. If K is small enough, then a Viterbi decoding will do. Otherwise, a sequential decoding procedure or its modification may be necessary.

References

[1] G. Solomon and H. C. A. van Tilborg, "A Connection Between Block and Convolutional Codes," *SIAM J. Appl. Math*, vol. 37, no. 2, pp. 358–369, October 1979.

[2] R. W. D. Booth, M. A. Herro, and G. Solomon, "Convolutional Coding Techniques for Certain Quadratic Residue Codes," *International Telemetering Conference (XI) Proceedings*, Silver Springs, Maryland, pp. 168–177, October 1975.

[3] G. Solomon and R. J. McEliece, "Weights of Cyclic Codes," *Journal of Combinatorial Theory*, vol. 1, no. 4, pp. 459–475, December 1966.